CalPERS

File Transport Service

- Encryption / Decryption (Internal)

Title	File Transport Service (FTS) - Encryption / Decryption (Internal)
Project	
Author	
Initiated On	
Filename	
Keywords	
Comments	
Last Saved By	
Last Saved On	

Revision History

Date	Version	Description	Author
02/26/07	0.1	Initial version	Mike Sisler
08/23/07	1.1	General Release	Shan Bains
08/10/08	2.0	Update revision	Shan Bains

1. INTRODUCTION

The File Transport Service (FTS) Encryption Decryption Service is designed to allow an external entity to interact with CalPERS using encrypted data files. The service allows both inbound and outbound transfer of files using standard PGP encryption. This document outlines the requirements for an external partner to utilize this service.

Internal Partner Requirements

Each internal application will be provided with two folders on an internal FTP CalPERS server. The first folder will be a prod-in folder for transfer of files TO CalPERS (inbound). The second folder will be a prod-out folder for transfer of files FROM CalPERS (outbound). The processing requirements are listed below.

Outbound files from CalPERS:

- A Public PGP key must be retrieved from the trading partner and placed on the appropriate key ring. Refer to the ISO key ring management document for these steps.
- The internal application will upload files to the prod-out folder on CalPERS internal ftp server using Binary mode.
- Data file names must be all lower case and must adhere to the file name convention described later tin this document.
- Two files must be uploaded for each transaction, one data file and one semaphore file. Data files will have a .dat / .xml file extension. Sempahore files will have a .sem file extension. The semaphore file will have the same name as the data file but with a .sem file extension. The semaphore file is an empty file that indicates that the data file is complete and ready for further processing. Example of a file pair of files sent for each transaction.
  "*filename*.dat and "*filename*".sem or "*filename*.xml and "*filename*".sem
- The CalPERS FTS Encryption Decryption Service will retrieve the data file and the semaphore files from the internal FTP location prod-out directory at a pre-determined interval.
- The data file and the semaphore file will be deleted from the internal FTP location prod-out directory after successful processing.
- An Email message will be sent when the files are successfully processed and delivered to the external FTP server trading partner location.
- Refer to the FTS Encryption Decryption (External) User Requirements.doc for further processing of outbound files to an external trading partner.

Inbound files to CalPERS:

- A CalPERS Public key must be sent to the trading partner prior to this process. Refer to the ISO key ring management document for these steps.
- Refer to the FTS Encryption Decryption (External) User Requirements.doc for pre-processing of inbound files from an external trading partner.
- Data file names will be all lower case.
- Two files will be sent to the prod-in directory for each inbound transaction, one data file and one semaphore file. Data files will have a .dat or .xml file extension. Sempahore files have a .sem file extension. The semaphore file is an empty file that indicates that the data file is complete and ready for further processing. Example of a file pair of files sent for each transaction. "*filename*.dat and "*filename*".sem or "*filename*.xml and "*filename*".sem
- The internal application will poll the internal FTP location at a pre-determined interval looking for files that are ready to be processed. Files are ready for processing when there is a pair of files with the same name but one has a .dat or .xml extension and one has a .sem extension. (see example above).
- The internal application will process the .dat / .xml file and then rename it to a .fin file extension. The renaming of the data file will indicate that the file has been processed and can be deleted by the FTS Encryption Decryption Cleanup Service.

File Naming Convention

Both inbound and outbound files must adhere to the file naming convention described below.

The standard format for file names:

A) ***yyyymmddhhmiss_sss_p(n).xxx***

Where:

yyyy is the year

mm is the month

dd is the day.

hh is the hours using a 24 hour clock

mi is the minutes

ss is the seconds

sss is the milliseconds, (use 000 if you cannot produce milliseconds)

p(n) application specific area of the file name (project defined)

xxx is the file extension (pgp) for all encrypted files
and .dat / .xml for data files